OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D. C. 20301-2000

POLICY

31 October 1989

Mr. John H. Wright
Information and Privacy Coordinator
Central Intelligence Agency
Washington, D.C. 20505

Dear Mr. Wright:

We appreciate your 4 October 1989 letter wherein suggested revisions were enclosed concerning Department of Defense (DoD) Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records."

Enclosed is a proposed revision to DoD Directive 5200.30 that contains your revisions and those from other agencies both within and outside of DoD.

Please provide us with your concurrence or comments by 29 December 1989.

My point of contact is Mr. Fred Cook, telephone 695-2686.

Sincerely,

Arthur E. Fajans
Director
Security Plans and Programs

STAT

Enclosure
As stated

Department of Defense
DIRECTIVE

NUMBER

SUBJECT: Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records

References: (a) DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," March 21, 1983 (hereby canceled)

(b) Executive Order 12356, "National Security Information," April 2, 1982

(c) Information Security Oversight Office Directive No. 1 Concerning National Security Information, June 23, 1982

(d) through (h), see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a); establishes procedures and assigns responsibilities for the systematic declassification review of information classified under references (b) and (c), DoD Directive 5200.1 and DoD 5200.1-R (references (d) and (e)), and prior orders, directives, and regulations governing security classification; and implements section 3.3 of reference (b).

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD) and to activities assigned to the OSD for administrative support, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

2. This Directive applies to the systematic review of permanently valuable classified information, developed by or for the Department of Defense and its Components, or its predecessor components and activities, that is under the exclusive or final original classification jurisdiction of the Department of Defense, and reference (f).

3. Its provisions do not cover Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954 (reference (g)) or information in nonpermanent records.

4. Systematic declassification review of records pertaining to intelligence activities (including special activities) or intelligence sources or methods shall ensure that all such records also be referred to the Central Intelligence Agency (CIA) for its determination, as the Director of Central Intelligence (DCI) is the sole statutory authority enjoined to protect intelligence sources and methods.

C. DEFINITIONS

1. Cryptologic Information. Information pertaining to or resulting from the activities and operations involved in the production of signals intelligence (SIGINT) or to the maintenance of information systems security (INFOSYSSEC).

2. Foreign Government Information. Information that is provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both are to be held in confidence; or produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof requiring that the information, the arrangement, or both are to be held in confidence.

3. Intelligence Method. Any process, mode of analysis, means of gathering data, or processing system or equipment used to produce intelligence.

4. Intelligence Source. A person or technical means that provides intelligence.

D. POLICY

It is the policy of the Department of Defense to assure that information that warrants protection against unauthorized disclosure is properly classified and safeguarded as well as to facilitate the flow of unclassified information about DoD operations to the public.

E. PROCEDURES

1. DoD classified information that is permanently valuable, as defined by 44 U.S.C. 2103 (reference (h)), that has been accessioned into the National Archives of the United States, will be reviewed systematically for declassification by the Archivist of the United States, with the assistance of the DoD personnel designated for that purpose, as it becomes 30 years old; however, file series concerning intelligence activities (including special activities) created after 1945, intelligence sources or methods created after 1945, and cryptology records created after 1945 will be reviewed as they become 50 years old. Any review of files concerning intelligence activities, sources, or methods shall include referral to the CIA.

2. All other DoD classified information and foreign government information that is permanently valuable and in the possession or control of DoD Components, including that held in federal records centers or other storage areas, may be reviewed systematically for declassification by the DoD Component exercising control of such information.

3. DoD classified information and foreign government information in the possession or control of DoD Components shall be declassified when they become 30 years old, or 50 years old in the case of DoD intelligence activities (including special activities) created after 1945, or cryptology created after 1945, if they are not within one of the categories specified in enclosure 2 or reference (f).

4. Systematic review for declassification shall be in accordance with procedures contained in DoD 5200.1-R (reference (e)). Information that falls within any of the categories in enclosure 2 and reference (f) shall be declassified if the designated DoD reviewer determines, in light of the declassification considerations contained in enclosure 3, that classification no longer is required. In the absence of such a declassification determination, the classification of the information shall continue as long as required by national security considerations.

5. Before any declassification or downgrading action, DoD information under review should be coordinated with the Department of State on subjects cited in enclosure 4, and with the CIA on subjects cited in enclosure 5.

F. RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Security Policy shall:

a. Exercise oversight and policy supervision over the implementation of this Directive.

b. Request DoD Components to review enclosures 2 and 3 of this Directive every 5 years.

c. Revise enclosures 2 and 3 to ensure they meet DoD needs.

d. Authorize, when appropriate, other federal agencies to apply this Directive to DoD information in their possession.

2. The Head of each DoD Component shall:

a. Recommend changes to the enclosures of this Directive.

b. Propose, with respect to specific programs, projects, and systems under his or her classification jurisdiction, supplements to enclosures 2 and 3 of this Directive.

c. Provide advice and designate experienced personnel to provide timely assistance to the Archivist of the United States in the systematic review of records under this Directive.

3. The Director, National Security Agency/Chief, Central Security Service (NSA/CSS), shall develop, for approval by the Secretary of Defense, special procedures for systematic review and declassification of classified cryptologic information.

4. The Archivist of the United States is authorized to apply this Directive when reviewing DoD classified information that has been accessioned into the Archives of the United States.

G. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures - 5

1. References
2. Categories of Information That Require Review Before Declassification
3. Declassification Considerations
4. Department of State Areas of Interest
5. Central Intelligence Agency Subjects of Special Concern

REFERENCES, continued

(d) DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982

(e) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982

(f) Title 32, Code of Federal Regulations, Part 2002, Information Security Oversight Office, "National Security Information; General Guidelines for Systematic Declassification Review of Foreign Government Information"

(g) Public Law 83-703, Atomic Energy Act of 1954

(h) Title 44, United States Code, Section 2103

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION

The following categories of information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive:

1. Nuclear propulsion information.

2. Information concerning the establishment, operation, and support of the U.S. Atomic Energy Detection System.

3. Information concerning the safeguarding of nuclear materials or facilities.

4. Information that could affect the conduct of current or future U.S. foreign relations. (Also see enclosure 4.)

5. Information that could affect the current or future military usefulness of policies, programs, weapon systems, operations, or plans when such information would reveal courses of action, concepts, tactics, or techniques that are used in current operations plans.

6. Research, development, test, and evaluation (RDT&E) of chemical and biological weapons and defensive systems; specific identification of chemical and biological agents and munitions; chemical and biological warfare plans; and U.S. vulnerability to chemical or biological warfare attack.

7. Information about capabilities, installations, exercises, research, development, testing and evaluation, plans, operations, procedures, techniques, organization, training, sensitive liaison and relationships, and equipment concerning psychological operations; escape, evasion, rescue and recovery, insertion, and infiltration and exfiltration; cover and support; deception; unconventional warfare and special operations; and the personnel assigned to or engaged in these activities.

8. Information that reveals sources or methods of intelligence or counterintelligence, counterintelligence activities, special activities, identities of clandestine human agents, methods of special operations, analytical techniques for the interpretation of intelligence data, and foreign intelligence reporting. This includes information that reveals the overall scope, processing rates, timeliness, and accuracy of intelligence systems and networks, including the means of interconnecting such systems and networks and their vulnerabilities.

9. Information that relates to intelligence activities conducted jointly by the Department of Defense with other federal agencies or to intelligence activities conducted by other federal agencies in which the Department of Defense has provided support. (Also see enclosure 5.)

10. Airborne radar and infrared imagery.

11. Information that reveals space system:

a. Design features, capabilities, and limitations (such as antijam characteristics, physical survivability features, command and control design details, design vulnerabilities, or vital parameters).

b. Concepts of operation, orbital characteristics, orbital support methods, network configurations, deployments, ground support facility locations, and force structure.

12. Information that reveals operational communications equipment and systems:

a. Electronic counter-countermeasures (ECCM) design features or performance capabilities.

b. Vulnerability and susceptibility to any or all types of electronic warfare.

13. Information concerning electronic intelligence, telemetry intelligence, and electronic warfare (electronic warfare support measures, electronic countermeasures (ECM), and ECCM) or related activities, including:

a. Information concerning or revealing nomenclatures, functions, technical characteristics, or descriptions of foreign communications and electronic equipment, its employment or deployment, and its association with weapon systems or military operations.

b. Information concerning or revealing the processes, techniques, operations, or scope of activities involved in acquiring, analyzing, and evaluating the above information, and the degree of success obtained.

14. Information concerning Department of the Army systems listed in attachment 1.

15. Information concerning Department of the Navy systems listed in attachment 2.

16. Information concerning Department of the Air Force systems listed in attachment 3.

17. Information concerning Defense Advanced Research Projects Agency Programs listed in attachment 4.

18. Cryptologic information (including cryptologic sources and methods). This includes information concerning or revealing the processes, techniques, operations, and scope of SIGINT comprising communications intelligence, electronics intelligence, and telemetry intelligence; and the cryptosecurity and emission security components of INFOSYSSEC, including the communications portion of cover and deception plans.

a. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

(1) Those that relate to COMSEC. In documentary form, they provide COMSEC guidance or information. Many COMSEC documents and materials are accountable under the Communications Security Material Control System. Examples are items bearing transmission security (TSEC) nomenclature and crypto keying material for use in enciphering communications and other COMSEC documentation such as National Telecommunications and Information Systems Security Instructions, National COMSEC/Emanations Security (EMSEC) Information Memoranda, National Telecommunications and Information Systems Security Policies, COMSEC Resources Program documents, COMSEC Equipment Engineering Bulletins, COMSEC Equipment System Descriptions, and COMSEC Technical Bulletins.

(2) Those that relate to SIGINT. These appear as reports in various formats that bear security classifications, sometimes followed by five-letter codewords (World War II's ULTRA, for example) and often carrying warning caveats such as "This document contains codeword material" and "Utmost secrecy is necessary..." Formats may appear as messages having addressees, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

(3) RDT&E reports and information that relate to either COMSEC or SIGINT.

b. Commonly used words that may help in identification of cryptologic documents and materials are "cipher," "code," "codeword," "communications intelligence" or "COMINT," "communications security" or "COMSEC," "cryptanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "electronic intelligence" or "ELINT," "electronic security," "encipher," "encode," "encrypt," "intercept," "key book," "signals intelligence" or "SIGINT," "signal security," and "TEMPEST."

Attachments - 3

1. Department of the Army Systems
2. Department of the Navy Systems
3. Department of the Air Force Systems
4. Defense Advanced Research Projects Agency Programs

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION

DEPARTMENT OF THE ARMY SYSTEMS

The following categories of Army information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive.

1. Ballistic Missile Defense (BMD) missile information, including the principle of operation of warheads (fuzing, arming, firing, and destruct operations); quality or reliability requirements; threat data; vulnerability; ECM and ECCM; details of design, assembly, and construction; and principle of operations.

2. BMD systems data, including the concept definition (tentative roles, threat definition, and analysis and effectiveness); detailed quantitative technical system description-revealing capabilities or unique weaknesses that are exploitable; overall assessment of specific threat-revealing vulnerability or capability; discrimination technology; and details of operational concepts.

3. BMD optics information that may provide signature characteristics of U.S. and United Kingdom ballistic weapons.

4. Shaped-charge technology.

5. Fleshettes.

6. M380 Beehive round.

7. Electromagnetic propulsion technology.

8. Space weapons concepts.

9. Radar-fuzing programs.

10. Guided projectiles technology.

11. ECM and ECCM to weapons systems.

12. Armor materials concepts, designs, or research.

13. 2.75-inch Rocket System.

14. Air Defense Command and Coordination System (AN/TSQ-51).

15. Airborne Target Acquisition and Fire Control System.

16. Chaparral Missile System.

17. Dragon Guided Missile System Surface Attack, M47.

18. Forward Area Alerting Radar (FAAR) System.

19. Ground laser designators.

20. Hawk Guided Missile System.

21. Heliborne, Laser, Air Defense Suppression and Fire and Forget Guided Missile System (HELLFIRE).

22. Honest John Missile System.

23. Lance Field Artillery Missile System.

24. Land Combat Support System (LCSS).

25. M22 (SS-11 ATGM) Guided Missile System, Helicopter Armament Subsystem.

26. Guided Missile System, Air Defense (NIKE HERCULES with Improved Capabilities with HIPAR and ANTIJAM Improvement).

27. Patriot Air Defense Missile System.

28. Pershing IA Guided Missile System.

29. Pershing II Guided Missile System.

30. Guided Missile System, Intercept Aerial M41 (REDEYE) and Associated Equipment.

31. U.S. Roland Missile System.

32. Sergeant Missile System (less warhead) (as pertains to electronics and penetration aids only).

33. Shillelagh Missile System.

34. Stinger/Stinger-Post Guided Missile System (FIM-92A).

35. Terminally Guided Warhead (TWG) for Multiple Launch Rocket System (MLRS).

36. TOW Heavy Antitank Weapon System.

37. Viper Light Antitank/Assault Weapon System.

CATEGORIES OF INFORMATION THAT REQUIRE SYSTEMATIC BEFORE DECLASSIFICATION:

DEPARTMENT OF THE NAVY

The following categories of Navy and Marine Corps information require review by the cognizant Department of the Navy Original Classification Authority (OCA), or by authorized officials of the DoD or National Archives of the United States using approved Department of the Navy detailed guidelines for continued security protection of classified information beyond 30 years:

A. Scientific, Technological, or Economic Matters Relating to the National Security:

1. Space systems.

2. Airborne radar and infrared imagery.

B. Military Weapons; the Vulnerabilities or Capabilities of Systems, Installations, or Projects Relating to the National Security; and United States Government Programs for Safeguarding Nuclear Materials or Facilities:

1. Naval nuclear propulsion information (NNPI). (Note: Unclassified NNPI also requires case-by-case review by the OCA prior to public release.)

2. All information that is uniquely applicable to nuclear-powered surface ships and submarines.

3. Information concerning the vulnerabilities of conventional surface ships protective systems; ship-silencing; operational characteristics related to performance; and all static electricity (SE), alternating magnetic (AM), and underwater electric potential (UEP) data.

4. Information concerning diesel submarines dealing with ship silencing; acoustic warfare systems data; details of operational assignments; general arrangements, drawings, and plans (SS-563 class hulls only); and SE, AM, and UEP data.

5. Information concerning mine warfare, mine performance, mine characteristics, mine sweeping, and mine countermeasures, including strategic and tactical minelaying and tactics and techniques against specific types of mines.

6. Information concerning the performance, doctrine, employment, and vulnerability to countermeasures of specified torpedoes and the SUBROC and ASROC missiles; and the radiated output of specified torpedo countermeasure devices.

7. Information concerning specified submarine and surface ship sonars.

8. Design performance and functional characteristics of specified guided missiles and projectiles, radars, acoustic equipments, and fire control systems.

C. Intelligence Activities (including special activities) or Intelligence Sources and Methods, Confidential Sources, and Related Matters:

1. Information that reveals sources or methods of intelligence or counterintelligence and related matters.

2. Information about intelligence capabilities, installations, exercises, research, development, testing and evaluation, plans, operations, procedures, techniques, organization, training, and related matters.

3. Information that deals with escape, evasion, rescue and recovery, insertion, and infiltration and exfiltration.

4. Information relating to intelligence activities conducted jointly within the Department of Defense and with other U.S. organizations or other countries.

5. Sound Surveillance System (SOSUS) data.

D. Communications and Electronics:

1. Operational communications equipment and systems.

2. Current electronic intelligence, telemetry intelligence, and electronic warfare or related matters.

3. The electronic countermeasures and electronic counter-countermeasures features and capabilities of any operational electronic equipments and electronic warfare systems still in service.

E. Crypotology:

1. Communications security (COMSEC) documents and cryptographic materials.

2. Signals intelligence (SIGINT).

3. Research, development, test, and evaluation information about COMSEC and SIGINT.

F. Foreign Relations or Foreign Activities of the United States, Military Plans and Operations, and Vulnerabilities or Capabilities of Plans Relating to the National Security:

1. Information which is internationally-sensitive and has been determined to affect adversely the current or future military usefulness of Department policies; plans, or operations when such information would reveal courses of action, concepts, tactics, or techniques that are used in current operations plans.

2. Information concerning Department of the Navy operations security countermeasures; unconventional warfare and special operations; psychological operations; long-term cover plans; special deception devices, techniques, and classified tactics; wartime reserve modes of Department of the Navy electronic and acoustic systems; and special warfare ordnance and vehicles having classified characteristics.

3. Military plans or operations dealing with the research, development, test and evaluation of chemical and biological weapons and defensive systems; the specific identification of chemical and biological agents and munitions; chemical and biological warfare plans; and U.S. vulnerability to chemical or biological warfare attack.

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION DEPARTMENT OF THE AIR FORCE SYSTEMS

The Department of the Air Force has determined that the categories identified in enclosure 2 of this Directive shall apply to Air Force information.

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY PROGRAMS

The following categories of DARPA information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive.

Basic and advanced research, exploratory development and test and evaluation information concerning:

a. Aerospace and strategic technology

b. Materials sciences

c. Electronic sciences

d. Directed energy systems

e. Information sciences and technology

f. Nuclear monitoring research

g. Tactical technology

h. Smart weapons and sensors

i. Armor/anti-armor technology

j. Defense advanced manufacturing technology

DECLASSIFICATION CONSIDERATIONS

1. Technological developments; widespread public knowledge of the subject matter; changes in military plans, operations, systems, or equipment; changes in the foreign relations or defense commitments of the United States; and similar events may bear upon the determination of whether information should be declassified. If the responsible DoD reviewer decides that, in view of such circumstances, the public disclosure of the information being reviewed no longer would result in damage to the national security, the information shall be declassified.

2. The following are examples of considerations that may be appropriate in deciding whether information in the categories listed in enclosure 2 may be declassified when it is reviewed:

a. The information no longer provides the United States a scientific, engineering, technical, operational, intelligence, strategic, or tactical advantage over other nations.

b. The operational military capability of the United States revealed by the information no longer constitutes a limitation on the effectiveness of the Armed Forces.

c. The information is pertinent to a system that no longer is used or relied on for the defense of the United States or its allies and does not disclose the capabilities or vulnerabilities of existing operational systems.

d. The program, project, or system information no longer reveals a current weakness or vulnerability.

e. The information pertains to a diplomatic initiative that has been abandoned or achieved and will no longer damage the foreign relations of the United States.

f. The information concerns foreign relations matters whose disclosure can no longer be expected to cause or increase international tension to the detriment of the national security of the United States.

3. Declassification of information which reveals the fact of or identity of a U.S. intelligence source, method, or capability, even when such source, method, or capability is no longer employed and even when disclosure of such source, method, or capability might appear not to cause damage to the national security or place a person in immediate jeopardy, shall be carried out only by the CIA. All such material shall be referred to CIA for its determination. The DCI is the sole statutory authority enjoined to protect intelligence sources and methods.

4. Declassification of information that may reveal the identities of clandestine human agents shall be accomplished only through referral of said information to the CIA for its determination.

5. The NSA/CSS is the sole authority for the review and declassification of classified cryptologic information. The procedures established by the NSA/CSS to facilitate the review and declassification of classified cryptologic information are:

a. COMSEC Documents and Materials

(1) If records or materials in this category are found in agency files that are not under COMSEC control, refer them to the senior COMSEC authority of the agency concerned or by appropriate channels to the following address:

Director
National Security Agency
ATTN: Director of Policy (Q4)
Fort George G. Meade, Maryland 20755

(2) If the COMSEC information has been incorporated into other documents by the receiving agency, referral to the NSA/CSS is necessary before declassification.

b. SIGINT Information

(1) If the SIGINT information is contained in a document or record originated by a DoD cryptologic organization, such as the NSA/CSS, and is in the files of a noncryptologic agency, such material will not be declassified if retained in accordance with an approved records disposition schedule. If the material must be retained, it shall be referred to the NSA/CSS for systematic review for declassification.

(2) If the SIGINT information has been incorporated by the receiving agency into documents it produces, referral to the NSA/CSS is necessary before any declassification.

DEPARTMENT OF STATE AREAS OF INTEREST

1. All messages in which the Department of State is either the originator or addressee.

2. Foreign government or international organization documents, except for communications on military subjects between U.S. military authorities and their counterparts.

3. Other documents which include:

   a. Statements of U.S. intent to defend, or not to defend, identifiable areas, or along identifiable lines, in any foreign country or region.

   b. Statements of U.S. intent militarily to attack in stated contingencies identifiable areas in any foreign country or region.

   c. Statements of U.S. policies or initiatives within collective security organizations (for example, North Atlantic Treaty Organization (NATO) and Organization of American States (OAS)).

   d. Agreements with foreign countries for the use of, or access to, military facilities.

e. Contingency plans insofar as they involve other countries the use of foreign bases, territory or airspace, or the use of chemical, biological, or nuclear weapons.

f. Defense surveys of foreign territories for purposes of basing or use in contingencies.

g. Reports documenting conversations with foreign officials, that is, foreign government information, which includes all information provided to the U.S. Government by a foreign nation or international body of nations, with the expectation that the U.S. Government will protect its confidentiality.

h. Additional guidance on foreign government information is contained in attachment 1.

i. Additional guidance on foreign government documents is contained in attachment 2.

FOREIGN GOVERNMENT INFORMATION

This section relates to information obtained in conversations with foreign government officials as distinct from foreign government document. An important responsibility in reviewing is to preserve our information gathering ability by protecting sources and by ensuring that information entrusted to us is held in confidence. Hence, it is usually preferable that material not be released quoting officials of other governments as the release might make them or others leery of entering into discussions with U.S. officials in the future. Examples of how this is used are:

Reports of statements and comments by foreign government officials, government policy positions expressed in confidence, second hand comments (i.e., "The French Ambassador told me that Turkish Ambassador said ...") and the like would not normally be released unless they are:

a) purely banal, (e.g., introductory remarkds, social coversation),

b) non-sensitive, (e.g., speeches and discussions in public places, arrangements for meetings, travel plans),

c) subjects are not or are no longer sensitive and release would have no impact on current issues and relations or on living persons and would not deter others from providing information.

-- An official's views might, be releasable if incorporated into U.S. reporting without named attribution, and the subject matter is no longer considered protectable.

-- If an official's comments are quoted in the public press, or in memoirs and such documents, there is no problem with their release. However, it is not feasbile for the reviewers to do complete research jobs.

-- The release of information might have an impact on the individual who gave it even though the material itself is not longer sensitive. In such cases, the material can be released and the source protected.

FOREIGN GOVERNMENT DOCUMENTS

The general rule is not to release foreign government documents provided in confidence unless such documents have since been released by the originating government or included in such published works as memoirs of senior officials of that government. It is not simply the substance of the document that is important but the process of communications. Other governments cannot be expected to respect the confidentiality of our communications if the U.S. is not willing to extend them the same respect. Even those governments which have Freedom of Information and historical document release programs, such as the U.K. and Canada, expect us to preserve the confidentiality of their documents until they make the decision to release them to their own public. Unless otherwise indicated, it should be assumed that every foreign government document is privileged even if the document does not bear a classification marking, and that unauthorized release reasonably could be expected to have a damaging effect on the foreign relations of the United States.

A gray area exists in the case of papers of defunct regimes, e.g., the Government of Vietnam, the Royal Laotian Government, the Imperial Government of Iran. If such documents are found in material that is being reviewed, consult the Department of State.

There may on occasion be exceptional circumstances, such as a court order to compel, in which the release of a foreign government document will be considered if the government which originated the document is consulted. In these cases, the Department of State should be requested to ask permission from the government involved.

Foreign government documents which have been transferred to and accessioned by the National Archives and Records Administration (NARA) are the responsibility of that agency.

CENTRAL INTELLIGENCE AGENCY--SUBJECTS OF SPECIAL CONCERN

1. Information that identifies CIA operational organizations, installations, agents, sources, or methods.

2. Information that could identify CIA personnel under official or nonofficial cover, or could reveal a cover arrangement.

3. Intelligence reports that could have come from covert sources, or information derived from them, which could divulge intelligence sources or methods.

4. Information the release of which could place an individual in jeopardy.

5. Information that could divulge intelligence interests, intelligence requirements, the value of intelligence information, or the extent of Intelligence Community knowledge on a subject.

6. Names of CIA staff personnel or agents.

7. Information divulging U.S. intelligence collection and assessment capabilities.

8. Information on technical systems for the collection or production of intelligence.

9. Methods or procedures used to acquire or produce intelligence or support intelligence activities.

10. Information on the structure, size, budget, foreign and domestic installations, security, or objectives of CIA.

11. Training provided to or by CIA personnel that would indicate CIA's capabilities or identify its personnel or agents.

12. CIA's personnel recruiting, hiring, training, assignment, and/or evaluation policies.

13. Any reports or publications by CIA, particularly NATIONAL INTELLIGENCE ESTIMATES, other finished intelligence analysis, raw (field) intelligence reports, and related documents.

14. Special access programs used by CIA.

15. Information on CIA's counterintelligence policies, practices, and capabilities.

16. Information on secret writing, including, e.g., specific chemicals, reagents, developers, and microdots.

17. Contractual relationships entered into by CIA, especially those which reveal specific interests and expertise.

18. Any CIA information or publication including or derived from SIGINT (COMINT, ELINT, etc.). [Material in this category should also be referred to NSA.]

19. Any CIA information or publication including or derived from overhead imagery.

20. Information on foreign nuclear programs, facilities, capabilities, or intentions.

21. Diplomatic or economic activities affecting the national security or international security negotiations.

22. Information related to political or economic instabilities in a foreign country, the divulgence of which could endanger American lives or installations in that country.

23. Covert activities conducted abroad in support of U.S. foreign policy.

24. Information on the surreptitious collection of information in a foreign nation by U.S. intelligence, especially when its disclosure could affect relations with that country.

25. Covert relationship with international organizations or foreign governments, especially liaison arrangements with foreign intelligence services and information derived from that liaison.

26. Information on the defense plans and capabilities of the U.S. or its allies, exposure of which could enable an adversary to develop counter-measures.

27. Information tending to disclose U.S. systems and weapons capabilities or deployment.

28. Information affecting U.S. plans to meet diplomatic contingencies affecting the national security.

29. Information the disclosure of which could lead to foreign political, economic, or military action against the United States of its allies.

30. Information on U.S. nuclear programs and facilities.

31. Information on research, development, and engineering that enables the United States to maintain an advantage of value to national security.